Microsoft

Microsoft Ignite
The Tour

Learn. Explore. Connect.

Microsoft

Risk Reduction for your Endpoints Using Microsoft Threat Protection

The cybersecurity landscape is rapidly changing

Cyberspace is the new battlefield

Security skills are in short supply

Virtually anything can be attacked

The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated attacks.

The digital estate offers a very broad surface area that is difficult to **secure**.

Integrated, intelligent correlation and action on signals is difficult, time-consuming, and **expensive**.

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

Outlook

400B emails analyzed

1.2B devices scanned each month

OneDrive

200+ global cloud consumer and commercial services

5B threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Windows

Botnet data from Microsoft Digital Crimes Unit

Microsoft accounts

Enterprise security for **90%** of Fortune 500

Azure

750M+ Azure user accounts

Xbox Live

18B+ Bing web pages scanned

Bing

450B monthly authentications

Microsoft Threat Protection

Identities

Users and Admins

Endpoints

Devices and Sensors

User Data

Email messages and documents

Cloud Apps

SaaS Applications and Data Stores

Infrastructure

Servers, Virtual Machines, Databases, Networks

Intelligent Security Graph
6.5 TRILLION signals per day

Microsoft Threat Protection

1. **Identities:** Validating, verifying and protecting both user and admin accounts
2. **Endpoints:** protecting user devices and signals from sensors
3. **User Data:** evaluating email messages and documents for malicious content
4. **Cloud Apps:** protecting SaaS applications and their associated data stores
5. **Infrastructure:** protecting servers, virtual machines, databases and networks across cloud and on-premises locations

Azure Active Directory	Azure Advanced Threat Protection	Microsoft Cloud App Security
Microsoft Intune	Windows 10	Azure Security Center
Windows Defender Advanced Threat Protection	Office 365 Advanced Threat Protection	Office 365 Threat Intelligence
Windows Server Linux	Exchange Online Protection	SQL Server

Microsoft Threat Protection solves your challenges

Today's security is multiple, disjointed, complex

Optimal security, minimal complexity

Microsoft Threat Protection solves your challenges

Microsoft Threat Protection

Optimal security, minimal complexity

Microsoft

The Next Generation of Threat & Vulnerability Management

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.

Security monitoring

Vulnerability management

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

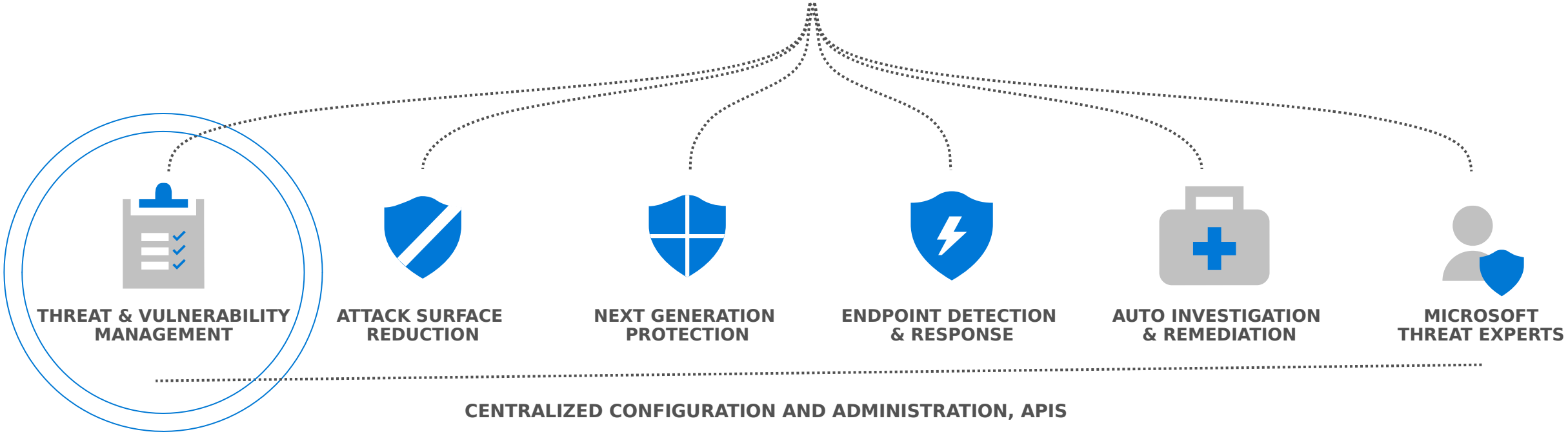
AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



Question

You have discovered 99 vulnerabilities in your environment - which should be prioritized first?

A. Affects the most hosts

B. Highest media attention

C. Most critical severity

Vulnerability Management (VM):

The process in which vulnerabilities in IT are **discovered** and the risks of these vulnerabilities are **evaluated**

Brief History

1990

SATAN
1st network vulnerability scanner
(replaced by NMAP & Nessus)

1995

Commercial VM
Network fingerprinting and banner grabbing

2000

Authenticated scanning
Enabled end point visibility & deep software analysis (e.g. ActiveX)

2005

Application aware
Identifying application security vulnerabilities and misconfigurations (e.g. CGI)

2010

Plugin ecosystem
Extending functionality via modules (e.g. Web Fuzzing)

2015

Technology coverage
Supporting Container, Cloud, Virtualization, IOT, Mobile, SCADA…

Today

Agent-Based
Continuous data collection

Key customers’ pain points

Discover

Periodic scanning

Blind spots

No run-time info

“Siloed modules”

Prioritize

Based on severity

No threat view

Missing org context

Large threat reports

Compensate

Waiting for a patch

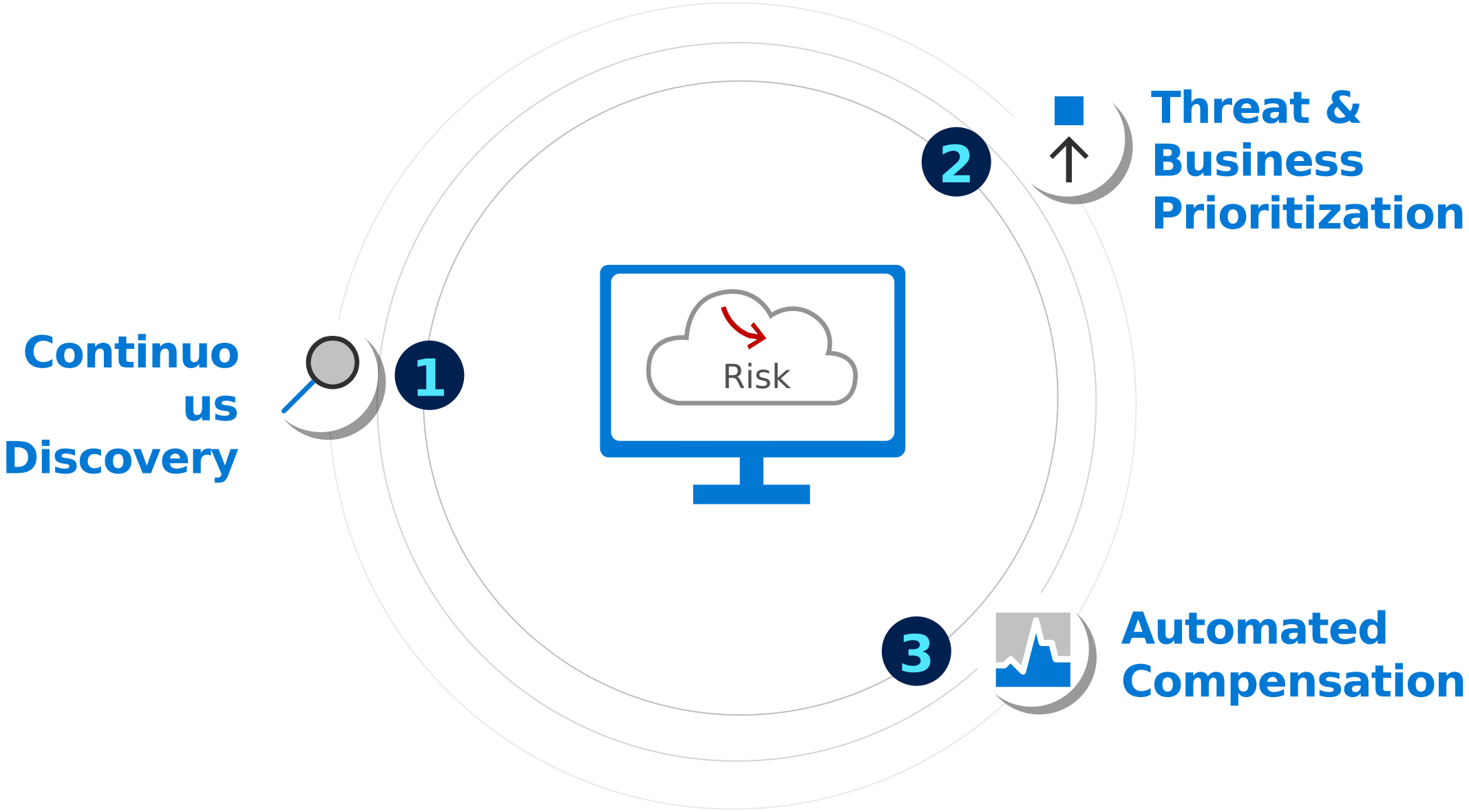
No IT/Security bridge

Manual process

No validation

Bottom line: Organizations remain highly vulnerable, despite high maintenance costs

Risk based approach to vulnerability management



1 Continuous Discovery

Extensive vulnerability assessment across the entire stack

Easiest to exploit

Application extension vulnerabilities

Application-specific vulnerabilities that relate to component within the application.

For example: Grammarly Chrome Extension (CVE-2018-6654)

Application run-time libraries vulnerabilities

Reside in a run-time libraries which is loaded by an application (dependency).

For example: Electron JS framework vulnerability (CVE-2018-1000136)

Application vulnerabilities (1st and 3rd party)

Discovered and exploited on a daily basis.

For example: 7-zip code execution (CVE-2018-10115)

OS kernel vulnerabilities

Becoming more and more popular in recent years due to OS exploit mitigation controls.

For example: Win32 elevation of privilege (CVE-2018-8233)

Hardware vulnerabilities (firmware)

Extremely hard to exploit, but can affect the root trust of the system.

For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

Hardest to discover

1 Continuous Discovery

Broad secure configuration assessment (secure score++)

Operation system misconfiguration

File Share Analysis

Security Stack configuration

OS baseline

Application misconfiguration

Least-privilege principle

Client/Server/Web application analysis

SSL/TLS Certificate assessment

Account misconfiguration

Password Policy

Permission Analysis

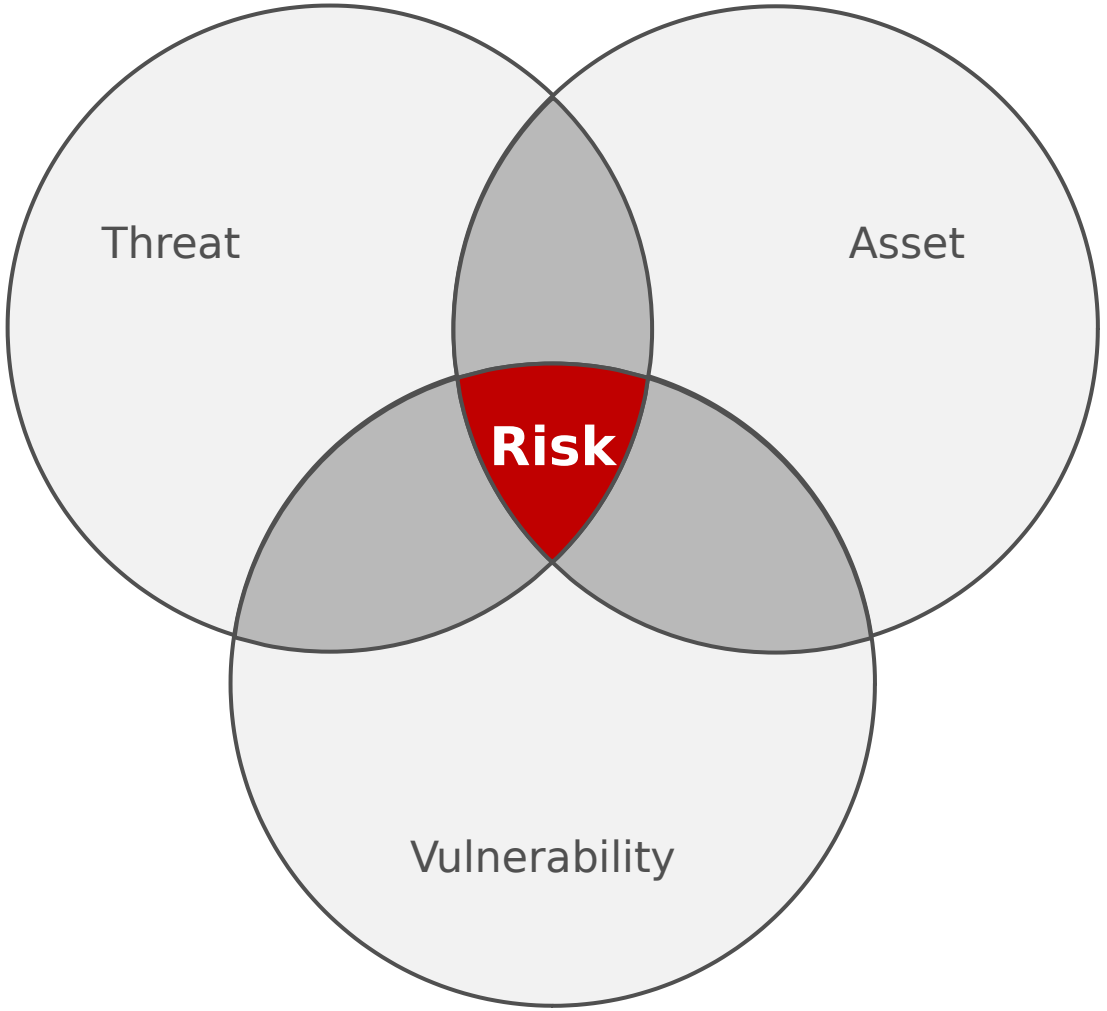
Network misconfiguration

Open ports analysis

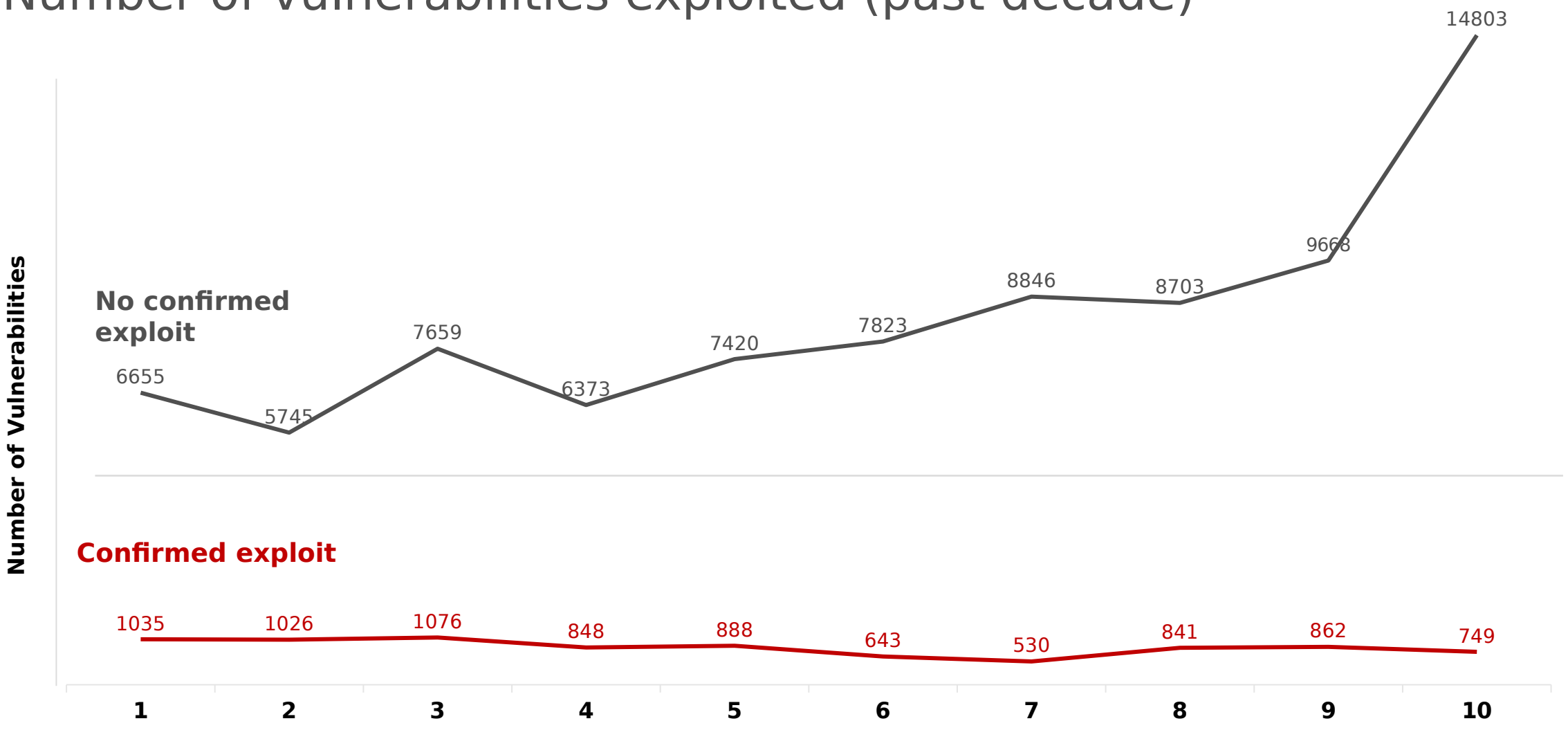
Network services analysis

WDATP TVM
Continuous Discovery Demo

Calculation of Associated Risk



Number of vulnerabilities exploited (past decade)

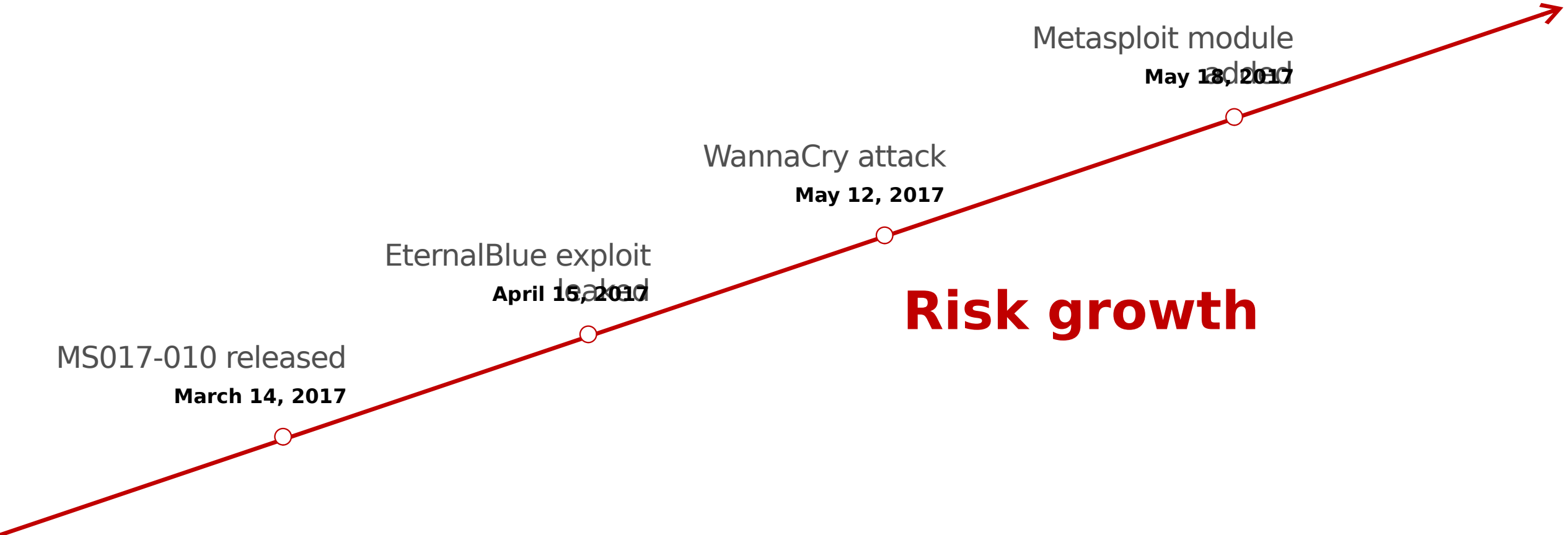


Source: IBM X-Force/Analysis: Gartner Research

Risk evolve over time

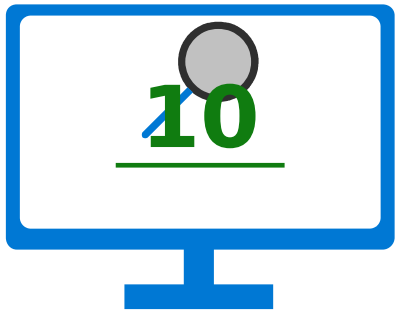
Vulnerabilities evolve over time as threat grows

Example: WannaCry ransomware campaign



2 Threat & Business Prioritization (“TLV”)

Helping customers focus on the right things at the right time



T

Threat Landscape

Vulnerability characteristics (CVSS score, days vulnerable)

Exploit characteristics (public exploit & difficulty, bundle)

EDR security alerts (Active alerts, breach history)

Threat analytics (live campaigns, threat actors)

L

Breach Likelihood

Current security posture

Internet facing

Exploit attempts in the org

V

Business Value

HVA analysis (WIP, HVU, critical process)

Run-time & Dependency analysis

WDATP TVM
Risk-Driven Prioritization
Demo

5 stages of mitigation grief

Denial

"These results are all false positives"

Anger

“This whole assessment effort is a waste of time”

Bargaining

“What’s the real risk? We have a compensating control..”

Depression

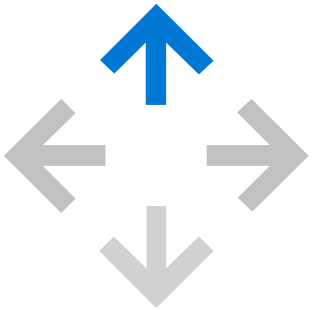
“I keep patching, but new vulnerabilities are killing me"

Acceptance

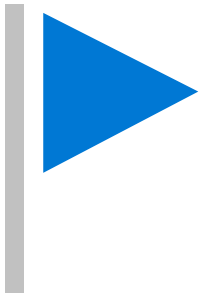
“It's going to be OK. I can't fight it”

Risk treatment

Remediation



Mitigation



Accept

3 Automated Compensation

Bridging between the IT and Security admins

Game changing IT/Security bridge scenarios

1-click remediation requests via Intune/SCCM

Automated task monitoring via run-time analysis

Tracking Mean-time-to-mitigate KPIs

Rich exception experience to mitigate/accept risk

Ticket management integration (Intune, Planner, Service Now, JIRA)

WDATP TVM
Risk Compensation
Demo

WDATP TVM
Putting it all together

Question

You have discovered 99 vulnerabilities in your environment - which should be prioritized first?

A. Affects the most hosts

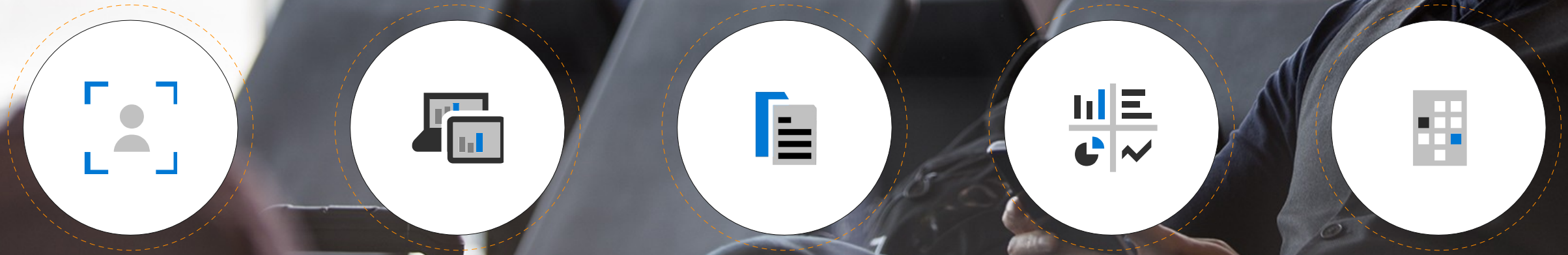
B. Highest media attention

C. Most critical severity

D. Highest risk exposure to the org

Microsoft Threat Protection

Microsoft Threat Protection



Identities

Users and admins

Endpoints

Devices and sensors

User Data

Email messages and documents

Cloud Apps

SaaS applications and data stores

Infrastructure

Servers, virtual machines, databases, networks

Optimal security with minimal complexity

Microsoft

© Copyright Microsoft Corporation. All rights reserved.